The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
3/30/2010

SUBJECT:
Multiple Vulnerabilities in Internet Explorer Could Allow Remote Code Execution (MS10-018)

OVERVIEW:
Ten vulnerabilities have been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. Exploitation may occur if a user visits or is redirected to a web page which is specifically crafted to take advantage of these vulnerabilities. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
- Windows 2000
- Windows 2003
- Windows XP
- Windows Vista
- Windows 7
- Windows Server 2008
- Internet Explorer 5
- Internet Explorer 6
- Internet Explorer 7
- Internet Explorer 8

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
Ten vulnerabilities have been discovered in Microsoft Internet Explorer. Details of these vulnerabilities are as follows:

Three Uninitialized Memory Corruption Vulnerabilities
Three remote code execution vulnerabilities exist in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. Exploitation may occur if a user visits or is redirected to a web page which is specifically crafted to take advantage of these vulnerabilities. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Please note that one of these three vulnerabilities (CVE-2010-0806) was originally discussed in CSCIC advisory number 2010-021. We have updated our advisory to reflect that this patch is now available and are issuing this advisory to discuss the entirety of the Microsoft out of band release MS10-018.

It is also important to note that if you applied the workarounds provided for CVE-2010-0806 then you must reverse them before applying the patch provided by Microsoft. Please follow the following instructions provided by Microsoft to reverse the workaround:

http://www.microsoft.com/technet/security/advisory/981374.mspx

Two HTML Object Memory Corruption Vulnerabilities
Two remote code execution vulnerabilities exist in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of these vulnerabilities. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Race Condition Memory Corruption Vulnerability
A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that may have been corrupted due to a race condition. Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of this vulnerability. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Memory Corruption Vulnerability
A remote code execution vulnerability exists in the way that Internet Explorer manages a long URL in certain situations. Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of this vulnerability. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

HTML Rendering Memory Corruption Vulnerability
A remote code execution vulnerability exists in the way that Internet Explorer accesses an object that has been deleted. Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of this vulnerability. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Post Encoding Information Disclosure Vulnerability
An information disclosure vulnerability exists in the way that Internet Explorer handles content using specific encoding strings when submitting data. Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of these vulnerabilities. Successful exploitation of this vulnerability could result in an attacker viewing content from the local computer or another browser window in another domain or Internet Explorer zone.

HTML Element Cross-Domain Vulnerability
An information disclosure vulnerability exists in Internet Explorer that could allow script to gain access to a browser window in another domain or Internet Explorer zone. Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of these vulnerabilities. Successful exploitation

of this vulnerability could result in an attacker viewing content from the local computer or another browser window in another domain or Internet Explorer zone.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

REFERENCES:
Microsoft:
http://www.microsoft.com/technet/security/bulletin/ms10-mar.mspx
http://www.microsoft.com/technet/security/bulletin/ms10-018.mspx
http://blogs.technet.com/msrc/archive/2010/03/29/internet-explorer-cumulative-update-releasing-out-of-band.aspx

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0267
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0488
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0489
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0490
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0491
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0492
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0494
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0805
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0806

Secunia:
http://secunia.com/advisories/38860